Beschreibung

Verfahren und Schaltungsanordnung zur geschützten Übertragung von Datenworten

Die Erfindung betrifft ein Verfahren und eine Schaltungsanordnung zur geschützten Übertragung von Datenworten gemäß den nebengeordneten Patentansprüchen.

Schaltungsanordnungen zur Datenverarbeitung umfassen im Wesentlichen ein Rechenwerk, einen Speicher sowie periphere Einheiten und einen Bus zum Datenaustausch zwischen dem Rechenwerk, dem Speicher und den peripheren Einheiten. Die Schaltungsanordnungen können in ihrer Funktionsweise durch Fehler in der Hardware oder externe Störquellen beeinträchtigt werden.

Bisherige Sicherheitskonzepte zum Schutz der Datenverarbeitung innerhalb einer Schaltungsanordnung konzentrieren sich darauf, lediglich einen Teil der Schaltungsanordnung zu schützen. Durch Vorsehen einer kryptografischen Einheit ist es beispielsweise möglich, Daten im Speicher vor dem nicht bestimmungsgemäßen Gebrauch bei unberechtigtem Auslesen zu schützen. Hierbei werden die im Speicher abzulegenden Daten vor dem Speichern verschlüsselt und beim Laden wieder entschlüsselt, sodass im Speicher die Daten nur in verschlüsselter Form vorliegen.

Eine weitere Schutzmöglichkeit ist die Verwendung fehlerkorrigierender Kodes. Hierbei werden einem Datenwort redundante Informationen hinzugefügt, durch die Änderungen einzelner Bits erkannt und korrigiert werden können. Fehlerkorrigierende Kodes können sowohl zum Schutz der Daten im Speicher als auch während der Datenübertragung, beispielsweise über den Bus, verwendet

werden. Die Datenübertragung über den Bus lässt sich auch durch eine Verschlüsselung der Daten während des Transfers absichern.

Bei den oben genannten Maßnahmen beschränkt sich der Schutz der Daten auf Bereiche der Schaltungsanordnung außerhalb des Rechenwerkes.

Angesichts neuer Angriffsszenarien, die lokale oder weiträumige Licht- oder Temperaturangriffe umfassen, gehen neue Sicherheitskonzepte dazu über, Fehler bei der Datenübertragung nicht mehr zu verhindern, sondern lediglich zu erkennen und eine geeignete Reaktion der Schaltungsanordnung anzustoßen.

Aufgabe der Erfindung ist, ein einfaches Verfahren zur gesicherten Datenübertragung bereit zu stellen, mittels dessen der gesamte Datenverkehr bis zum Rechenwerk überprüft werden kann, sowie eine geeignete Schaltungsanordnung.

Die Aufgabe wird durch die in den nebengeordneten Patentansprüchen angegebenen Maßnahmen gelöst.

Das Verfahren zur geschützten Übertragung von Datenworten umfasst ein Bereitstellen eines ersten Datenwortes, eine Transformation des ersten Datenwortes in eine Sequenz aus mindestens einem zweiten Datenwort durch eine erste Transformationsregel, eine Transformation zumindest eines der zweiten Datenworte in ein drittes Datenwort durch eine zweite Transformationsregel und ein Überprüfen, ob zwischen dem dritten Datenwort und einem Vergleichsdatenwort ein vorgegebener Zusammenhang besteht.

Außerdem ist eine Schaltungsanordnung zur geschützten Übertragung von Datenworten angegeben, die für den Einsatz des genannten Verfahrens geeignet ist.

Wesentliche Komponenten einer Schaltungsanordnung zur eigentlichen Datenverarbeitung sind ein Speicher und ein Rechenwerk. Im Speicher liegt der auszuführende Programmkode als eine Folge von Datenworten vor, die Daten und Instruktionen umfassen. Ein Satz möglicher Instruktionen, aus denen die Datenworte des Programmkodes gewählt sind, ist meist so gewählt, dass er nicht nur von einer bestimmten Rechenwerksarchitektur verarbeitet werden kann, sondern in unterschiedlichen Schaltungsanordnungen oder Rechenwerken einsetzbar ist.

Die Datenworte des Programmkodes können vom Rechenwerk nicht direkt verarbeitet werden, da das Rechenwerk über einen eigenen Befehlsatz verfügt, der meist hinsichtlich der Rechenwerksarchitektur oder häufiger Anforderungen optimiert ist. Dieser Befehlssatz des Rechenwerkes unterscheidet sich von dem möglichst flexiblen und vielen Anforderungen gerecht zu werdenden Befehlssatz der Programmdaten. Deswegen ist eine erste Transformationseinrichtung, die auch als Dekoder bezeichnet wird, vorgesehen, um die ersten Datenworte der Programmdaten in speziell auf das Rechenwerk angepasste zweite Datenworte zu übertragen. Die zweiten Datenworte sind Befehlsworte für das Rechenwerk. Jedes erste Datenwort wird in eine Sequenz von Datenworten übertragen, die ein oder mehrere zweite Datenworte umfasst. Die von der ersten Transformationseinrichtung ausgegebenen zweiten Datenworte werden vom Rechenwerk verarbeitet.

Die zweiten Datenworte werden speziell für das Rechenwerk generiert, das die zweiten Datenworte zu verarbeiten hat. Es gibt Rechenwerke, für die ein erstes Datenwort in eine Sequenz mit genau einem zweiten Datenwort übertragen wird. Es gibt Rechenwerke, für die ein erstes Datenwort in eine Sequenz mit mehreren zweiten Datenworten übertragen wird. Dabei ist es selbstver-

ständlich denkbar, dass für einige erste Datenworte die resultierende Sequenz nur ein zweites Datenwort umfasst. Bei letztgenannten Rechenwerken handelt es sich in der Regel um einfache und flexible Rechenwerke.

Der Vorteil des Verfahrens ist, dass nicht in die eigentliche Datenverarbeitung der ersten, beziehungsweise zweiten Datenworte eingegriffen wird. Vielmehr dienen die zweiten Datenworte gleichzeitig als Kontrollinformation der ersten Datenworte, denen sie zu Grunde liegen. Es wird überprüft, ob die ersten und zweiten Datenworte nach der Datenübertragung noch zusammenpassen. Wenn dieses nicht der Fall ist, ist von einem Fehler in der Datenübertragung auszugehen, der möglicherweise auf einem Angriff beruht.

Die ersten und zweiten Datenworte werden an geeigneten Stellen der Schaltungsanordnung abgegriffen. Geeigneten Stellen sind vorzugsweise vor und nach der ersten Transformationseinrichtung, die die ersten Datenworte in die zweiten Datenworte überführt. Das zweite Datenwort wird, wie im Folgenden beschrieben, überprüft, ob es mit einem Vergleichsdatenwort in einem gegebenen Zusammenhang steht.

Der Dekoder kann auch mehrstufig ausgeführt sein. Zwischen den Dekoderstufen ist ein Abgriff der zweiten Datenworte denkbar. Die erste Transformationseinrichtung entspricht in diesem Fall den Dekoderstufen zwischen den Abgriffen. Ebenso ist es denkbar, dass die erste Transformationseinrichtung mehrere Dekoder umfasst, die nacheinandergeschaltet sind. Vor und/oder nach den Abgriffen können weitere Dekoder vorgesehen sein. Die erste Transformationsregel bezieht sich dann auf die zwischen den Abgriffen durchgeführten Transformationen. Durch Wahl des Abgriff kann zwischen Aufwand und Schutzbereich abgewogen werden.

Zur Überprüfung wird das zweite Datenwort einer zweiten Transformation unterzogen. Die zweite Transformation ist so gewählt, dass deren Ergebnis mit einem Vergleichsdatenwort übereinstimmt, wenn bei der Übertragung kein Fehler aufgetreten ist. Bei dem Vergleichsdatenwort handelt es sich vorteilhafterweise um das erste Datenwort. Es ist auch denkbar, dass das dritte Datenwort und das Vergleichsdatenwort in einem gegebenen Zusammenhang stehen. Invertierung oder Shiften sind denkbare Zusammenhänge, ebenso wie die Übereinstimmung ausgewählter Bitpositionen innerhalb der Datenworte. Letzteres ist allerdings kein eineindeutiger Zusammenhang zwischen zwei Datenworten. Ein Satz von Datenworten kann diesen Zusammenhang erfüllen. Für die Fehlererkennung ist es allerdings von Vorteil, wenn der Zusammenhang so gegeben ist, dass einem Datenwort in eindeutiger Weise das Vergleichsdatenwort zugeordnet ist.

Wenn jedes erste Datenwort bei der ersten Transformation in eine Sequenz mit genau einem zweiten Datenwort überführt wird, umfasst das Verfahren in Regel zueinander inverse erste und zweite Transformationen, wenn das Vergleichsdatenwort das erste Datenwort ist.

Wird bei der Dekodierung aus dem ersten Datenwort eine Sequenz von mehreren zweiten Datenworten generiert, so lässt sich anhand nur eines dieser zweiten Datenworte häufig nicht eindeutig rückschließen, welchem ersten Datenwort das zweite Datenwort zuzuordnen ist. Auf Grund der einfacheren Struktur des Rechenwerkes ist dessen Befehlssatz häufig kleiner als der Satz von möglichen ersten Datenworten. Folglich ist dasselbe zweite Datenwort Teil verschiedener Sequenzen, die sich bei der Transformation verschiedner erster Datenworte ergeben. Ein einzelnes zweites Datenwort innerhalb der Sequenz erlaubt keinen Rückschluss mehr

auf das zu Grunde liegende erste Datenwort. Mehrere erste Datenworte können in Frage kommen. Deshalb kann das Ergebnis der zweiten Transformation eines zweiten Datenwortes, das unabhängig von den übrigen zweiten Datenworten der Sequenz betrachtet wird, einen Satz mit möglichen ersten Datenwort umfassen, zu denen das zweite Datenwort gehören kann. Da bereits bei der ersten Transformation der eindeutige Zusammenhang zwischen einen einzigen zweiten Datenwort und dem zu Grunde liegenden ersten Datenwort verloren gegangen ist, ist dieser Zusammenhang auch nach der zweiten Transformation des zweiten Datenwortes nicht gegeben. Somit stehen die ersten und dritten Datenworte nicht mehr in einem eindeutigen Zusammenhang. Vielmehr besteht dann ein Zusammenhang zwischen einem dritten Datenwort und mehreren ersten Datenwörtern.

Zum besseren Schutz ist es wünschenswert, dass das Ergebnis der zweiten Transformation eindeutig auf das erste Datenwort, das dem zweiten Datenwort zugeordnet ist, zurück schließen lässt. Deshalb werden vorteilhafterweise den generierten zweiten Datenworten zusätzliche Informationen hinzugefügt, aus denen hervorgeht, aus welchem ersten Datenwort das zweite Datenwort transformiert worden ist. Diese Vorgehen ist sinnvoll, wenn das zweite Datenwort innerhalb einer Sequenz mit mehreren zweiten Datenworten ist, die aus dem ersten Datenwort überführt worden ist. Zweite Datenworte, die innerhalb mehrerer möglicher Sequenzen vorkommen, lassen sich infolgedessen losgelöst von der Sequenz stets dem dieser Sequenz zu Grunde liegendem ersten Datenwort zuordnen. Damit kann auch nach einer zweiten Transformation ein eindeutiger Zusammenhang zwischen ersten und drittem Datenwort gewährleistet sein.

Häufig bereitet die schaltungstechnische Realisierung der zweiten Transformationsregel als Umkehrtransformation der ersten

Transformationsregel Schwierigkeiten. In diesem Fall wird die zweite Transformation nur als eine teilweise Umkehrung der ersten Transformation ausgestaltet. Als Ergebnis der zweiten Transformation liegt dann nicht das ursprüngliche erste Datenwort vor, sondern ein drittes Datenwort. Um das dritte Datenwort mit dem ersten Datenwort vergleichen zu können, wird das erste Datenwort ebenfalls transformiert. Eine dafür verwendete dritte Transformation ist so zu wählen, dass ihr Ergebnis mit dem Ergebnis der ersten Transformation samt der daran anschließenden teilweise Umkehrung dieser durch die zweite Transformation übereinstimmt beziehungsweise zum Vergleichsdatenwort führt, das in dem gegebenen Zusammenhang mit dem dritten Datenwort steht.

Eine auf dem oben geschilderten Verfahren basierende Schaltungsanordnung umfasst neben der herkömmlichen Schaltungsanordnung zur Datenverarbeitung weitere Blöcke. Die erste Transformationseinrichtung überführt das erste Datenwort in das zweite Datenwort oder in die Sequenz von zweiten Datenworten. Vorteilhafterweise wird vor dem Rechenwerk das zweite Datenwort abgegriffen und mittels einer zweiten Transformationseinrichtung in das dritte Datenwort überführt, das mit dem ersten Datenwort verglichen werden kann. Dazu dient eine Prüfungseinrichtung.

Falls die zweite Transformationseinrichtung keine gänzliche Umkehrung der ersten Transformation ermöglicht, ist zwischen dem Speicher und der Prüfungseinrichtung eine dritte Transformationseinrichtung vorzusehen, sodass die dritte Transformationseinrichtung und die Aneinanderschaltung der ersten und zweiten Transformationseinrichtung jeweils ein Datenwort liefern, die dahingehend geprüft werden können, ob der gegebene Zusammenhang besteht.

Wenn das erste, gegebenenfalls transformierte, Datenwort und das dritte Datenwort nicht übereinstimmen, führt die Prüfungseinrichtung eine Alarmfunktion, beispielsweise ein Alarmsignal, aus.

Weitere vorteilhafte Ausgestaltungen der Erfindung sind in den untergeordneten Patentansprüchen angegeben.

Nachfolgend wird die Erfindung unter Bezugnahme auf die Zeichnung anhand von Ausführungsbeispielen erklärt.

Es zeigen:

Figur 1 ein erstes Ausführungsbeispiel eines Verfahrens zur geschützten Übertragung von Datenworten,

Figur 2 ein weiteres Ausführungsbeispiel des Verfahrens zur geschützten Übertragung von Datenworten,

Figur 3 noch ein weiteres Ausführungsbeispiel des Verfahrens zur geschützten Übertragung von Datenworten,

Figur 4 ein Ausführungsbeispiel einer Schaltungsanordnung zur geschützten Übertragung von Datenworten und

Figur 5 ein weiteres Ausführungsbeispiel der Schaltungsanordnung zur geschützten Übertragung von Datenworten.

Figur 1 zeigt ein einfaches Ausführungsbeispiel eines Verfahrens, um ein erstes Datenwort X1, das in ein zweites Datenwort X2 überführt wird, zu überprüfen.

Zunächst sei der prinzipielle Ablauf des erfindungsgemäßen Verfahrens anhand dieses einfachen Ausführungsbeispiels dargestellt. Aus einem ersten Datenwort X1 wird über eine erste Transformation T1 eine Sequenz S2 von Datenworten generiert. Im dargestellten Fall umfasst die Sequenz S2 genau ein zweites Datenwort X2.

Das zweite Datenwort X2 wird über eine zweite Transformation T2 in ein drittes Datenwort X3 überführt. Dabei besteht zwischen dem dritten Datenwort X3 und dem ersten Datenwort X1 ein vorgegebener Zusammenhang. Im Idealfall bedeutet „vorgegebener Zusammenhang", dass das dritte Datenwort X3 mit dem ersten Datenwort X1 identisch ist. Dies ist der Fall, wenn die zweite Transformation T2 eine Umkehrtransformation der ersten Transformation T1 ist.

In einer Überprüfung K wird geprüft, ob zwischen dem dritten Datenwort X3 und einem Vergleichsdatenwort VX ein vorgegebener Zusammenhang besteht. In diesem Fall ist das Vergleichsdatenwort VX das erste Datenwort X1. Wenn es sich bei der zweiten Transformation T2 um die Umkehrfunktion der ersten Transformation T1 handelt, handelt es sich hierbei um eine Prüfung auf Identität des ersten Datenwortes X1 und des dritten Datenwortes X3. Falls das dritte Datenwort X3 und das erste Datenwort X1 nicht in gegebenen Zusammenhang stehen, beziehungsweise diese Datenworte nicht identisch sind, wird eine Alarmfunktion ALARM durchgeführt.

Die Alarmfunktion ALARM kann vielfältig sein und hängt auch von der Verwendung des Verfahrens ab. Ausführungen hierzu finden sich in der Beschreibung der Schaltungsanordnung.

Figur 2 zeigt ein weiteres Ausführungsbeispiel des Verfahrens zur geschützten Übertragung von Datenworten. Das erste Datenwort X1 wird in diesem Fall durch die erste Transformation T1 in eine Sequenz S2 von mehreren zweiten Datenworten X2 transformiert.

In diesen Fällen ist nicht mehr unbedingt jedes einzelne der zweiten Datenworte X2 der Sequenz S2 eindeutig dem ersten Datenwort X1 zuordenbar. Da der für das Rechenwerk bestimmte Satz an möglichen Datenworten kleiner ist, werden dieselben zweiten Datenworte X2 in verschiedenen möglichen Sequenzen S2 verwandt, die jeweils einem ersten Datenwort X1 zugeordnet sind. Das bedeutet, nicht mehr ein einzelnes Datenwort X2 ist dem ersten Datenwort X1 eindeutig zugeordnet, sondern die Sequenz S2 mit mehreren zweiten Datenworten X2 als Ganzes.

Abhängig vom ersten Datenwort X1 kann die Anzahl der zweiten Datenworte X2 in der entsprechenden Sequenz S2 variieren. Es ist auch denkbar, dass die Sequenz S2 nur ein einziges zweites Datenwort X2 umfasst.

Mit der zweiten Transformation T2 wird jedes der zweiten Datenworte X2 in ein drittes Datenwort X3 überführt. Es ist nicht gewährleistet ist, dass aus einem einzelnen, zweiten Datenwort X2 innerhalb der Sequenz S2 auf das erste Datenwort X1 zurück zu schließen ist. Deshalb stehen nach der zweiten Transformation T2 das erste und eines der dritten Datenworte X3 nicht unbedingt in einem eindeutigen Zusammenhang. Aus einem dritten Datenwort X3 lässt sich nicht unbedingt auf das zu Grunde liegende erste Datenwort X1 schließen. Es ist jedoch beispielsweise möglich, aus dem dritten Datenwort X3 auf einen Satz von möglichen ersten Datenworten X1 zu schließen. In diesem Fall ist die Fehlererkennung eingeschränkt. In der Prüfung K wird dann geprüft, ob das ursprüngliche erste Datenwort X1 im Satz möglicher erster Daten-

worte, der sich nach der zweiten Transformation T2 ergibt, enthalten ist. Wenn dieses nicht der Fall ist, lässt das auf einen Fehler schließen. Wenn der Satz möglicher erster Datenworte dagegen das ursprüngliche erste Datenwort X1 umfasst, sind zwei Möglichkeiten denkbar. Die Übertragung war fehlerfrei, oder wenn es bei der Übertragung zu einem Fehler gekommen ist, so hat dieser zu einem Satz möglicher erster Datenworte geführt, der ebenfalls das ursprüngliche erste Datenwort X1 umfasst.

Ein Beispiel soll die Problematik verdeutlichen. Es wird angenommen, dass im Programmkode ein Befehl „ADD-SHIFT" als erstes Datenwort X1 vorgesehen ist. „ADD-SHIFT" addiert zwei Registeradressen und verschiebt die resultierende Adresse um ein Bit. Des Weiteren sei ein Befehl „ADD-LOAD" als weiteres erstes Datenwort X1 vorgesehen, bei dem zwei Registeradressen addiert werden und die resultierende Adresse an das System gegeben wird, um von dieser Adresse ein Datum zu laden. Bei der ersten Transformation T1 wird der Befehl „ADD-SHIFT" in eine Sequenz S2 mit einem „ADD"-Befehl und einem „SHIFT"-Befehl als zweiten Datenworten X2 überführt. Der Befehl „ADD-LOAD" wird in eine Sequenz S2 mit einem „ADD"-Befehl und einem „LOAD"-Befehl als zweiten Datenworten X2 überführt. Bei beiden Sequenzen S2 tritt zunächst der „ADD"-Befehl als erstes der zweiten Datenworte X2 auf. Betrachtet man lediglich dieses zweite Datenwort X2 der beiden Sequenzen S2, ist nicht zu unterscheiden, ob das zu Grunde liegende erste Datenwort X1 der Befehl „ADD-SHIFT" oder „ADD-LOAD" ist. Nur aus „ADD" lässt nicht auf das erste Datenwort X1 rückschließen. Das zweite Datenwort X2 kann entweder vom ersten Datenwort „ADD-SHIFT" oder vom ersten Datenwort „ADD-LOAD" stammen. Bei diesem Beispiel lässt sich aus „ADD" nur auf einen Fehler schließen, wenn das erste Datenwort X1 weder „ADD-SHIFT" noch „ADD-LOAD" ist.

Um die Sicherheit des Verfahrens zu erhöhen, wird jedem zweiten Datenwort X2 nach der ersten Transformation T1 Information I zugeordnet, sodass das resultierende zweite Datenwort X2 eindeutig dem ersten Datenwort X1 zuordenbar ist.

Im oben genannten Beispiel wird beispielsweise dem zweiten Datenwort X2 „ADD" ein Bit, „0" oder „1", hinzugefügt, aus dem hervorgeht, ob das erste Datenwort X1 ein „ADD-SHIFT"- oder ein „ADD-LOAD"-Befehl ist. Beispielsweise wird ein „ADD0" in ein „ADD-SHIFT" transformiert und ein „ADD1" in ein „ADD-LOAD". Jedes der dritten Datenworte X3 steht somit eindeutig mit dem zu Grunde liegenden ersten Datenwort X1 in gegebenem Zusammenhang. Damit ist es auch möglich, mit der zweiten Transformation T2 ein drittes Datenwort X3 auszugeben, das eindeutig dem ersten Datenwort X1 zuordenbar ist. In der Überprüfung K wird der gegebene Zusammenhang geprüft. Wenn der Zusammenhang nicht gegeben ist, wird eine Alarmfunktion ALARM durchgeführt.

Vorteilhafterweise sind die dritten Datenworte X3 mit dem ersten Datenwort X1 identisch. Da aus einem ersten Datenwort X1 über verschiedenen zweite Datenworte X2 identische dritte Datenworte X3 generiert werden, handelt es sich bei der zweiten Transformation T2 nicht um eine eineindeutige Abbildung. Auch in diesem Ausführungsbeispiel ist das erste Datenwort X1 das Vergleichsdatenwort VX.

Wegen der Sicherheit sollte, jedes zweite Datenwort X2 der Sequenz S2 in ein jeweiliges drittes Datenwort X3 überführt werden, die mit dem entsprechenden Vergleichsdatenwort VX, hier das erste Datenwort X1, verglichen werden. Es ist aber auch denkbar, nur einen Teil der zweiten Datenworte X2 der zweiten Transformation T2 zu unterziehen und zu überprüfen.

Figur 3 stellt eine weitere Ausgestaltung des Verfahrens dar. Es unterscheidet sich von dem Verfahren gemäß Figur 2 durch eine dritte Transformation im Zweig zwischen dem ersten Datenwort X1 und der Überprüfung K. Deshalb wird im Folgenden nur auf die Unterschiede eingegangen.

In diesem Ausführungsbeispiel wird die zweite Transformation T2 so gewählt, dass es sich hierbei nicht um eine Umkehrtransformation der ersten Transformation T1 handelt. In diesem Fall stimmen die dritten Datenworte X3 nicht mit dem ersten Datenwort X1 überein. Um dennoch eine Überprüfung K hinsichtlich der Identität durchführen zu können, wird das erste Datenwort X1 einer dritten Transformation T3 unterzogen. Die dritte Transformation T3 ist so gewählt, dass sie das gleiche Ergebnis liefert wie die Aneinanderreihung der ersten und zweiten Transformation T1, T2.

Im Extremfall können die erste, zweite und dritte Transformation T1, T2, T3 so gewählt werden, dass es sich bei der zweiten Transformation T2 um die Identität handelt, d. h. das Eingang und Ausgang der Transformation gleich sind. Dies wäre gleichbedeutend mit dem Weglassen des Kreises T2 in der Figur 3. In diesem Fall handelt es sich bei der ersten und dritten Transformation T1, T3 um die gleiche Abbildung, wenn die Überprüfung K auf Identität erfolgt.

Figur 4 zeigt eine Schaltungsanordnung, in der das beschriebene Verfahren Anwendung findet. Die Schaltungsanordnung umfasst einen Speicher MEM und ein Rechenwerk CPU. Es sei bemerkt, dass es sich bei dem Speicher MEM auch um einen Zwischenspeicher handeln kann, der einem eigentlichen Hauptspeicher nachgeschaltet ist.

Zur Anpassung der im Speicher MEM zur Datenverarbeitung bereitgestellten ersten Datenworte X1 ist eine erste Transformations-

einrichtung DEC vorgesehen, die die ersten Datenworte X1 eines Programmkodes an den Befehlssatz des Rechenwerks CPU anpasst. Dieses entspricht der oben geschilderten ersten Transformation T1. Die Architektur des Rechenwerkes und der ersten Transformationseinrichtung DEC kann entweder so gewählt sein, dass es sich um eine so genannte RISC-Architektur handelt, bei der jedem ersten Datenwort X1 eine Sequenz S2 mit genau einem zweiten Datenwort X2 zugeordnet wird. Es kann sich auch um eine CISC-Architektur handeln, bei der das erste Datenwort X1 in eine Sequenz S2 von mehreren zweiten Datenworten X2 überführt wird. Die Anzahl der zweiten Datenworte X2 in der Sequenz S2 kann variieren. Auch eine Sequenz S2 mit nur einem zweiten Datenwort X2 ist hierbei denkbar.

Die Daten werden aus dem Speicher MEM über mehrere Pufferstufen geladen. In Figur 4 sind beispielhaft eine erste Pufferstufe 1 und eine zweite Pufferstufe 2 dargestellt, die der ersten Transformationseinrichtung DEC vor- und nachgeschaltet sind. Die erste Puffereinrichtung 1 stellt die ersten Datenworte X1 für die erste Transformationseinrichtung DEC zur Verfügung. Aus der zweiten Pufferstufe 2 werden die zweiten Datenworte X2 für das nachgeschaltete Rechenwerk CPU zur eigentlichen Verarbeitung bereitgestellt. Entlang des beschriebene Weges erfolgt die eigentliche Datenverarbeitung der Datenworte vom Speicher MEM zum Rechenwerk CPU. Es wäre auch ein direkter Abgriff des ersten und zweiten Datenwortes X1, X2 vor beziehungsweise nach der ersten Transformationseinrichtung DEC denkbar. Die Abgriffe können auch unmittelbar nach dem Speicher MEM und/oder vor oder gar durch das Rechenwerk CPU erfolgen. Der geschützte Bereich hängt von der Wahl der Abgriffe entlang des Datenübertragungsweges ab.

Um zu kontrollieren, ob das für das Rechenwerk CPU bereitgestellte zweite Datenwort X2 in der zweiten Puffereinrichtung 2

korrekt ist, oder auf dem Weg dorthin manipuliert worden ist, ist eine zweite Transformationseinrichtung R1 und eine Prüfungseinrichtung COMP vorgesehen. Die Prüfungseinrichtung COMP ist sowohl über die zweite Transformationseinrichtung R1 an den zweiten Puffer 2 als auch an den ersten Puffer 1 gekoppelt. Die zweite Transformationseinrichtung R1 ist ausgebildet das zweite Datenwort X2 in das dritte Datenwort X2 zu überführen.

Die Prüfungseinrichtung COMP ist ausgebildet, ein anliegendes Datenwort und ein anliegendes Vergleichsdatenwort VX miteinander hinsichtlich eines gegebenen Zusammenhanges zu überprüfen. In der Regel handelt es sich hierbei um einen Vergleich auf Identität des anliegenden dritten Datenwortes X3 und des ersten Datenwortes X1 als Vergleichsdatenwort VX. Wenn die beiden zu überprüfenden Datenworte nicht identisch beziehungsweise in definierter Weise verknüpft sind, wird eine Alarmfunktion ALARM durchgeführt.

In der zweiten Transformationseinrichtung R1 wird das Datenwort aus dem zweiten Puffer 2 transformiert. Diese Transformation entspricht der zweiten Transformation T2. Sie ist vorteilhafterweise so gewählt, dass es sich hierbei um eine Umkehrfunktion der von der ersten Transformationseinrichtung DEC bereitgestellten ersten Transformation T1 handelt. Wenn es zu keinem Angriff oder Übertragungsfehler gekommen ist, ist das dritte Datenwort X3, das ausgangsseitig an der zweiten Transformationseinrichtung R1 anliegt und auf die Prüfungseinrichtung COMP gegeben wird, identisch mit dem ersten Datenwort X1. Im Falle von, zufälligen oder durch Manipulationen hervorgerufenen, Datenfehlern stehen das erste und dritte Datenwort X1, X3 nicht mehr in gegebenem Zusammenhang, da die Fehler im Rahmen der ersten und/oder zweiten Transformationen T1, T2 zu Folgefehlern führen oder bei der Transformation selbst durch den Angriff verursacht werden. Da

die erste und zweite Transformation T1, T2 sich unterscheiden, ist es schwierig, den Angriff so zu gestalten, dass beide Transformationen in aufeinander abgestimmte Weise manipuliert werden, dass Datenveränderungen unbemerkt bleiben oder deren Folgen sich bei den Transformationen aufheben. Bei einem ausgedehntem Angriff, beispielsweise durch Licht, liefern beide Transformation unterschiedlichen Fehler, die beim Vergleich detektiert werden.

Figur 5 unterscheidet sich von Figur 4 lediglich darin, dass zwischen den ersten Puffer 1 und die Prüfungseinrichtung COMP eine dritte Transformationseinrichtung R2 gekoppelt ist. Im Folgenden wird nur auf die Unterschiede eingegangen.

Die Realisierung der hardwaretechnischen Umsetzung der Umkehrfunktion in der zweiten Transformationseinrichtung R1 gestaltet sich häufig schwierig. In diesen Fällen ist es nicht möglich, die zweite Transformationseinrichtung R1 derart auszubilden, dass an deren Ausgang wieder das ursprüngliche erste Datenwort X1 anliegt. In solchen Fällen wird nur eine teilweise Umkehrtransformation in der zweiten Transformationseinrichtung R1 durchgeführt, deren Ergebnis das dritte Datenwort X3 ist. Der noch ausstehende Teil der Umkehrfunktion wird in den Pfad zwischen dem ersten Puffer 1 und der Prüfungseinrichtung COMP verlagert. Hierfür ist die dritte Transformationseinrichtung R2 vorgesehen. R2 ist derart ausgebildet, dass damit die dritte Transformation T3 realisiert wird. Damit liegt am Ausgang von der dritten Transformationseinrichtung R2 idealerweise das gleiche Datenwort an wie am Ausgang der zweiten Transformationseinrichtung R1. Alternativ können die Datenworte auch in einem anderen, gegebenen Zusammenhang stehen. Diese Datenworte werden in der Prüfungseinrichtung COMP miteinander verglichen.

Im Extremfall kann die zweite Transformationseinrichtung R1 sehr einfach ausgestaltet sein oder ganz wegfallen, sodass der zweite Puffer 2 direkt mit der Prüfungseinrichtung COMP verbunden wäre. Dies entspricht der Identität als zweiter Transformation T2. In solchen Fällen ist die dritte Transformation T3, die von der dritten Transformationseinrichtung R2 bereitgestellt wird, vorteilhafterweise gleich mit der ersten Transformation T1, die in der ersten Transformationseinrichtung DEC ausgeführt wird. Auf zwei Pfaden wird folglich die gleich Transformation ausgeführt. Diese Ausgestaltung der Schaltungsanordnung hat den Nachteil, dass natürlich ein identischer Angriff auf zwei identisch funktionierende Einrichtungen erfolgen kann, der zu gleichen Fehlern führt, sodass die Manipulation in der Prüfungseinrichtung COMP unentdeckt bliebe. Bei den zuvor beschriebenen Ausführungen sind zwei oder gar drei verschiedene Transformationseinrichtungen DEC, R1, R2 vorgesehen, auf die unterschiedliche, aufeinander abgestimmte Angriffe erfolgen müssten, damit diese Angriffe unentdeckt blieben.

Die erste Transformationseinrichtung DEC und die zweite Transformationseinrichtung R1 sowohl in Figur 4 als auch in Figur 5 können vorteilhafterweise derart ausgestaltet sein, dass das resultierende dritte Datenwort X3 eindeutig zuordenbar ist oder nicht eindeutig zuordenbar ist. Letzteres ist oft der Fall, wenn das erste Datenwort X1 von der ersten Transformationseinrichtung DEC in eine Sequenz S2 zweiter Datenworte X2 überführt wird.

Wenn das dritte Datenwort X3 nicht eindeutig zuordenbar ist, also mehrere mögliche erste Datenworte dem dritten Datenwort X3 zuordenbar sind, wird in der Prüfungseinrichtung COMP lediglich festgestellt, ob die Zuordnung schlüssig ist. Alternativ ist die erste Transformationseinrichtung DEC, beispielsweise durch eine interne Einrichtung 3,derart ausgestaltet, dass Information I zu

dem zweiten Datenwort X2 hinzugefügt wird, sodass das erste Datenwort X1 und das Vergleichsdatenwort VX, sei es das erste Datenwort X1 oder dessen transformierte Form X1', in eindeutigen Zusammenhang gestellt werden können. In diesem Fall liefert die zweite Transformationseinrichtung R1 auch ein drittes Datenwort X3, das eindeutig dem ersten Datenwort X1 beziehungsweise dessen transformierter Form X1' am Ausgang der dritten Transformationseinrichtung R2 entspricht. Es ist auch denkbar, dass die Information I durch eine separate Einrichtung, gekoppelt mit oder parallel zur ersten Transformationseinrichtung DEC bereitgestellt wird.

Hinsichtlich der Reaktion der Schaltungsanordnung auf eine gegebenenfalls auszuführende Alarmfunktion ALARM sei bemerkt, dass diese vielfältig sein können. Sie hängen sowohl vom Sicherheitskonzept als auch von der Architektur der Schaltungsanordnung ab. Denkbar sind beispielsweise eine Ausgabe eines Alarmsignals, ein Herunterfahren der Schaltungsanordnung, ein Herunterfahren und erneutes Wiederhochfahren der Schaltungsanordnung oder eine wiederholte Datenverarbeitung des fehlerhaften Datenwortes.

Des Weiteren sei bemerkt, dass das erfindungsgemäße Verfahren nicht nur auf konventionelle Schaltungsanordnungen zur eigentlichen Datenverarbeitung beschränkt ist. Es ist auch denkbar, damit den Zugriff auf eine Speichereinrichtung abzusichern. In diesem Fall wird überprüft, ob das angeforderte Datenwort im Wege der Anforderung und des Hochladens manipuliert worden ist.

Patentansprüche

1. Verfahren zur geschützten Übertragung von Datenworten umfassend

- Bereitstellen eines ersten Datenwortes (X1),

- Transformation des ersten Datenwortes (X1) in eine Sequenz aus mindestens einem zweiten Datenwort (X2) durch eine erste Transformationsregel (T1),

- Transformation zumindest eines der zweiten Datenworte (X2) in ein drittes Datenwort (X3) durch eine zweite Transformationsregel (T2),

- Überprüfen, ob zwischen dem dritten Datenwort (X3) und einem Vergleichsdatenwort (VX) ein vorgegebener Zusammenhang besteht.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass eine Alarmfunktion (ALARM) ausgeführt wird, wenn zwischen dem dritten Datenwort (X3) und dem Vergleichsdatenwort (VX) nicht der vorgegebene Zusammenhang besteht.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass vor der Transformation des zweiten Datenwortes (X2) dieses derart modifiziert wird, dass zwischen dem dritten Datenwort (X3) und dem Vergleichsdatenwort (VX) ein eindeutiger Zusammenhang besteht.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, dass das Modifizieren des zweiten Datenwortes (X2) ein Hinzufügen von Information (I) umfasst.

5. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass zwischen dem dritten Datenwort (X3) und dem Vergleichsdatenwort (VX) ein eindeutiger Zusammenhang besteht.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass der eindeutige Zusammenhang die Identität von dem dritten Datenwort (X3) mit dem Vergleichsdatenwort (VX) ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das erste Datenwort (X1) das Vergleichsdatenwort (VX) ist.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die zweite Transformationsregel (T2) eine Umkehrabbildung der ersten Transformationsregel (T1) ist.

9. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das erste Datenwort (X1) durch eine dritte Transformationsregel (T3) zum Vergleichsdatenwort (VX) transformiert wird.

10. Verfahren nach Anspruch 9, dadurch gekennzeichnet, dass das Ergebnis der dritten Transformationsregel (T3) angewendet auf das erste Datenwort (X1) im vorgegebenen Zusammenhang steht mit dem Ergebnis der Anwendung der zweiten Transformationsregel (T2) nach der ersten Transformationsregel (T1) auf das erste Datenwort (X1).

11. Verfahren nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass die zweite Transformationsregel (T2) die Identität ist und die erste und dritte Transformationsregel (T1, T3) gleich sind.

12. Schaltungsanordnung zur geschützten Übertragung von Datenworten mit

- einem Dateneingang, der mit einer ersten Transformationseinrichtung (DEC) verbunden ist, die ein erstes Datenwort (X1), das am Dateneingang anliegt, in eine Sequenz (S2) aus Datenworten transformiert, die mindestens ein zweites Datenwort (X2) umfasst,

- einer zweiten Transformationseinrichtung (R1), die an die erste Transformationseinrichtung (DEC) gekoppelt ist und die zumindest eines der zweiten Datenworte (X2) in ein drittes Datenwort (X3) transformiert,

- eine Überprüfungsseinrichtung (COMP), der das dritte Datenwort (X3) und ein Vergleichsdatenwort (VX) zugeführt werden, und die überprüft, ob das dritte Datenwort (X3) und das Vergleichsdatenwort (VX) in einem vorgegebenem Zusammenhang stehen.

13. Schaltungsanordnung nach Anspruch 12, dadurch gekennzeichnet, dass sie eine Alarmfunktion durchführt (ALARM), wenn das dritte Datenwort (X3) und das Vergleichsdatenwort (VX) nicht in dem vorgegebenem Zusammenhang stehen.

14. Schaltungsanordnung nach einem der Ansprüche 12 bis 13, dadurch gekennzeichnet, dass das erste Datenwort (X1) als Vergleichsdatenwort (VX) der Prüfungseinrichtung (COMP) zugeführt wird.

15. Schaltungsanordnung nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, dass eine Einrichtung vorgesehen ist, die das zweiten Datenwort (X2) derart modifiziert, dass der vorgege-

bene Zusammenhang zwischen dem Vergleichsdatenwort (VX) und dem dritten Datenwort (X3) eindeutig ist.

16. Schaltungsanordnung nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, dass die erste Transformationseinrichtung (DEC) das zweite Datenwort (X2) derart modifiziert, dass der vorgegebene Zusammenhang zwischen dem Vergleichsdatenwort (VX) und dem dritten Datenwort (X3) eindeutig ist.

17. Schaltungsanordnung nach einem der Ansprüche 12 bis 16, dadurch gekennzeichnet, dass eine dritte Transformationseinrichtung (R2) vorgesehen ist, die der Überprüfungseinrichtung (COMP) vorgeschaltet ist und die das eingangsseitig anliegende erste Datenwort (X1) in das Vergleichsdatenwort (VX) transformiert.

18. Schaltungsanordnung nach Anspruch 17, dadurch gekennzeichnet, dass die zweite Transformationseinrichtung (R1) derart ausgebildet ist, dass das dritte Datenwort (X3) mit dem zweiten Datenwort (X2) übereinstimmt.

19. Schaltungsanordnung nach Anspruch 17, dadurch gekennzeichnet, dass die erste und dritte Transformationseinrichtung (DEC, R2) die gleiche Transformation ausführen.

20. Schaltungsanordnung nach einem der Ansprüche 12 bis 19, dadurch gekennzeichnet, dass der vorgegebene Zusammenhang die Identität von dem Vergleichsdatenwort (VX) und dem dritten Datenwort (X3) ist.

21. Schaltungsanordnung nach einem der Ansprüche 12 bis 20, dadurch gekennzeichnet, dass die erste Transformationseinrichtung (DEC) zwischen einem Rechenwerk (CPU) und einer Speichereinrichtung (MEM) angeordnet ist.

22. Schaltungsanordnung nach einem der Ansprüche 12 bis 21, dadurch gekennzeichnet, dass der ersten Transformationseinrichtung (DEC) mindestens eine weitere Transformationseinrichtung vor- und/oder nachgeschaltet ist.

Zusammenfassung

Verfahren und Schaltungsanordnung zur geschützten Übertragung von Datenworten

Ein Verfahren zur geschützten Übertragung von Datenworten umfasst ein Bereitstellen eines ersten Datenwortes (X1), eine Transformation des ersten Datenwortes (X1) in eine Sequenz aus mindestens einem zweiten Datenwort (X2) durch eine erste Transformationsregel (T1), eine Transformation zumindest eines der zweiten Datenworte (X2) in ein drittes Datenwort (X3) durch eine zweite Transformationsregel (T2), und ein Überprüfen, ob zwischen dem dritten Datenwort (X3) und einem Vergleichsdatenwort (VX) ein vorgegebener Zusammenhang besteht.

Figur 1

Bezugszeichenliste

X1	erstes Datenwort
X1'	transformiertes erstes Datenwort
X2	zweites Datenwort
X3	drittes Datenwort
VX	Vergleichsdatenwort
S2	Sequenz
I	Zusatzinformation
T1	erste Transformation
T2	zweite Transformation
T3	dritte Transformation
K	Vergleich
MEM	Speicher
CPU	Rechenwerk
DEC	erste Transformationseinrichtung
R1	zweite Transformationseinrichtung
R2	dritte Transformationseinrichtung
COMP	Prüfungseinrichtung
1	erster Puffer
2	zweiter Puffer
3	interne Einheit
ALARM	Alarmfunktion